

AMVIA Data Services Acceptable Use Policy

This Acceptable Use Policy forms part of the Agreement between Amvia and the Customer and applies to data, internet access, hosted network and related connectivity services supplied or supported by Amvia.

The purpose of this Policy is to protect Amvia, its customers, supplier networks and the wider internet community from unlawful, harmful, abusive, insecure or operationally disruptive use of the services.

Introduction

Use of any relevant service by the Customer constitutes acceptance of this Policy, as amended from time to time in accordance with the Agreement.

This Policy is intended to define prohibited behaviour, set minimum expectations for secure and lawful use, and explain how suspected abuse, misuse or policy breaches may be reported and handled.

This Policy should be read together with the Agreement, Order, service schedule and any applicable technical, security or usage documentation. Where there is any inconsistency, the Agreement and Order take precedence unless they expressly state that this Policy overrides them.

Prohibited Use

The Customer must not use, and must ensure that its users, employees, contractors and anyone using the services through the Customer do not use, the services for any unlawful, harmful, fraudulent, abusive or operationally disruptive purpose.

Without limitation, the following are prohibited:

- Impersonation, forgery or spoofing, including adding, removing or modifying identifying network header information in order to deceive, mislead or impersonate another person or system.
- Attempting to gain unauthorised access to any electronic systems, networks, applications or data, whether or not the attempt is successful.
- Threats of bodily harm, destruction of property, threatening conduct or harassment.
- Use of the services for any illegal purpose.
- Resale of any service without proper authorisation from Amvia.
- Publication, storage, transmission or distribution of material that infringes intellectual property rights or copyright, unless the Customer has the necessary ownership, permissions or releases.

The Customer must ensure that its use of the services is consistent with applicable law, regulatory requirements, contractual obligations and generally accepted standards of responsible internet use.

Network Use

The Customer must not engage in any activity that adversely affects the ability of other people, systems or networks to use Amvia services or the internet.

This includes denial of service activity, interference with or disruption of network services or equipment, hostile traffic generation, propagation of malicious or abusive traffic, and any conduct that degrades network performance, security or availability for others.

The Customer is responsible for ensuring that its own environment is configured and maintained in a secure manner. The Customer must not, through action or inaction, permit its systems, network, devices or credentials to be used by third parties for illegal, abusive or inappropriate activity.

If insecure configuration, poor access control, malware compromise, open services or unmanaged exposure creates a material risk to Amvia or others, Amvia may require remedial action and may suspend or restrict the affected service where reasonably necessary.

Email and Messaging

Amvia does not tolerate or endorse e-mail spamming or the sending of unsolicited commercial e-mail through, from or using the services.

The Customer must not send large volumes of unsolicited e-mail, whether commercial or otherwise, and must not use an Amvia e-mail address, domain, hosted service or web presence to collect responses generated by unsolicited communications.

Where the Customer carries out legitimate marketing or bulk messaging activity, it must do so lawfully and responsibly, including using appropriate consent standards such as double opt-in where required, maintaining opt-out mechanisms, and ensuring that recipients are aware why they are receiving the communication.

The Customer must not facilitate spam or abusive e-mail activity, and any mail servers operated by or for the Customer must not be configured as open relays.

Anonymous bulk e-mailing is prohibited. If complaints, technical impact or third-party reports indicate abusive e-mail behaviour, Amvia may take immediate action, including restriction, suspension or termination of affected services or accounts.

Content and Platforms

The Customer must not use an Amvia-hosted website, web account, platform, mailbox, domain, application environment or related service for the distribution of illegal material or to support unlawful conduct.

The Customer must not use an Amvia web address, hosted account or related service to collect responses from unsolicited commercial e-mail or to facilitate abusive marketing practices.

The Customer must not advertise, transmit, provide or otherwise make available any software, service, tool or process designed to breach this Policy or the acceptable use policy of another provider, including software or services intended to facilitate spam or similar abuse.

Where the services support news, forum or community posting functions, the Customer must use good judgement, comply with applicable group rules and avoid off-topic posting, excessive multi-posting, hostile posting or cancellation of messages belonging to others except where forged in the Customer's own name.

Capacity and Resource Use

The Customer must not use bandwidth, storage, platform resources or related service capacity in excess of agreed limits or in a way that materially affects Amvia's wholesale carriers' ability to provide services to others.

Where limits are expressly defined in the applicable service description, order or account specification, those limits apply. Where limits are not expressly defined, Amvia may determine reasonable operational limits by reference to technical performance, normal usage patterns, service stability and the need to protect the wider platform.

If Amvia reasonably determines that excessive bandwidth, storage or related resource consumption is adversely affecting service delivery, Amvia may take immediate protective action and will attempt to notify the Customer as soon as reasonably practicable.

Cooperation and Reporting

The Customer must cooperate with Amvia in investigating suspected misuse, abuse, copyright complaints, security incidents, spam, scanning activity, attempted system penetration, malware activity or other suspicious conduct connected with the services.

Reports of suspected abuse should be directed to Amvia's abuse contact address at abuse@amvia.co.uk

Where a report is made, the reporting party should provide, where available, the IP address involved, the date and time of the alleged incident including time zone or GMT offset, and supporting evidence such as full e-mail headers, firewall logs, syslog records or equivalent technical evidence.

Amvia may use abuse reports and related information to investigate incidents, enforce this Policy, improve filtering or security controls and support cooperation with relevant authorities or rights holders where appropriate.

Enforcement

If Amvia reasonably believes that this Policy has been breached, Amvia may take proportionate action to protect its services, customers, suppliers or third parties.

Such action may include one or more of the following:

- Issuing a verbal or written warning.
- Requiring the Customer to take corrective action within a specified time.
- Suspending specific functions, posting privileges, accounts or affected services.
- Restricting traffic, blocking content, isolating systems or applying technical controls to contain the issue.
- Terminating the affected service or the Agreement for material or repeated breach.
- Charging the Customer for reasonable administrative, remediation, reactivation or third-party costs arising from the breach where permitted by the Agreement.

Amvia will generally seek to act reasonably and proportionately, but may act immediately and without prior notice where urgent action is necessary to protect systems, networks, users, suppliers or the public.

General

Capitalised terms used in this Policy but not defined in it have the meanings given in the Agreement or applicable Order.

Amvia may review and amend this Policy from time to time on written notice where reasonably necessary to reflect changes in law, regulation, threat landscape, supplier obligations, platform design, service scope or operational requirements.

This Policy should be read together with the relevant Amvia service schedule, security documentation, tariff documentation and the main Agreement.